Depositor Guidance for the Transfer of Archival Born Digital Records

Version 3.0

February 2024

Preserving the past **l** Recording the present **l** Informing the future

Document Control

Title	Depositor Guidance for the Transfer of Archival Born Digital Records
Prepared By	Eve Wright, Digital Archivist
Approved By	Laura Mitchell, Director of Information and Records Services and Deputy Keeper of the Records of Scotland
Date of Approval	27/02/2023
Version Number	3.0
Review Frequency	Bi-annually, or when process changes are implemented
Next Review Date	TBC January 2025

Document Owner

The document is owned by:

Name	Role	Team / Branch	Directorate
Eve Wright	Digital Archivist	Digital Records Unit	Information and Records Services

Status Control

Version	Issue Date	Status	Prepared By	Role	Reason for Amendment
1.1	April 2022	Draft	Eve Wright	Digital Archivist	Clearer structure
1.2	January 2023	Draft	Eve Wright	Digital Archivist	Inclusion of MFT guidance
1.3	January 2023	Draft	Eve Wright	Digital Archivist	Revision following comments from reviewers
2.0	February 2023	Draft	Eve Wright	Digital Archivist	Revision following comments from reviewers
3.0	February 2024	Final	Eve Wright	Digital Archivist	Slight change to terminology

Document Reviewers

The document is required to be reviewed by:

Name (Person / Board)	Role	Sign-off Required(Y/N)
Garth Stewart	**Head of Digital Records Unit**	N
Tim Gollins	**Head of Preservation and Information Management**	N
Susan Corrigall	**Head of Preservation**	N
Gillian Mapstone	**Head of Archive Depositor Liaison**	N
Laura Mitchell	**Director of Information and Records Services**	Y

Distribution List

This document has been distributed to:

Name (Person / Team)	Role	Issue Date	Version
Various	Depositors of born digital archival records to NRS	06/02/2024	3.0

Contents

1.   INTRODUCTION

This guidance describes the transfer of **born-digital records selected for permanent preservation** to National Records of Scotland (NRS).

Born digital records provide their own unique challenges in terms of transfer and preservation. In combination with support from your NRS Client Manager, this document will outline what Depositors and NRS need to do to ensure born digital records can be transferred to, and preserved by, NRS.

2.   DIGITAL PRESERVATION AT NRS

NRS has been accepting born digital records since 1998. Our Digital Repository (managed by NRS's Digital Records Unit) allows archival records to be stored and managed in an environment where preservation and security are paramount. NRS provides the technical expertise and dedicated resources required to ensure long-term preservation of records, administering checks and actions that may not be in place in the record creators' own IT systems. These steps are essential to preserve and protect the reliability, integrity, authenticity, and usability of these archival records, so that they can be accessed by future generations.

3.   FIRST STEPS

As part of transferring records to NRS for permanent preservation, you will work closely with your NRS Client Manager from our Archive Depositor Liaison team. They will talk you through the processes to follow for records to be transferred to NRS:

Appraisal and Selection	Records are examined and selected for permanent preservation based on their archival value. This process may take place over several meetings so that your Client Manager has a complete picture of what is to be transferred.
Establish Archive Deposit Agreement	This agreement sets out the understanding of the process of depositing, storing, preserving, and accessing the records and will be signed by both parties.
Sensitivity Review	A review of record content to determine if there is material that would be considered 'sensitive' in a data protection, freedom of information (exemption), or commercial sense. Information identifying the nature of the sensitivity of the records will need be included as part of the transfer of records (see section 4.4 'Manifest'): this must be completed by the Depositor ahead of the transfer and discussed with your Client Manager. Further guidance on sensitivity review (as well as what to do when redactions are required) can be found in Appendix A.

Where the transfer of records involves any born digital material (whether it be solely digital or a hybrid of analogue and digital records), your Client Manager will include

the Digital Records Unit (DRU) in transfer discussions. We will provide technical guidance and support for the entire transfer process.

3.1   Your Recordkeeping System

One of the first questions we ask our Depositors is:

- what system is currently being used to store the records in question?; and
- how easy is it to export the records from this system?

Broadly, record-keeping systems sit within three categories:

Type	Description	Examples
Directory or File System	System is not the record. Stores the record but does not describe it.	PC, hard drive, or shared drive.
Records Management System	System is not the record, but it can describe records within. Can link to local or cloud-based storage.	Microsoft OneDrive, SharePoint, Objective, Google Drive, bespoke EDRMS.
"Line of Business" System	System is the record, or it is part of it.	Databases, CMS, Finance or HR systems, eDiscovery.

NRS will be preserving the records themselves and not the system they are currently stored in. Therefore, some preparation may be required to anticipate this by the Depositor, often working in conjunction with their IT department.

The DRU will provide guidance on export and preparation ahead of transfer, based on the Depositor's situation.

3.2   Understanding file formats

It will be helpful for us to know at the outset if your organisation routinely creates files within proprietary systems, or which may otherwise have characteristics which present a challenge to preservation. The DRU will ask what types of records you will be depositing and discuss any potential preservation risks with you.

Please do not pre-emptively transform digital records you plan to transfer to us into any other format after their creation and use, without discussing this with us first.

There are a small number of file formats that we typically do not accept. These can be found in Appendix B.

4.   PREPARING FOR TRANSFER TO NRS

Pre-transfer, there is some essential preparation work required of the Depositor to ensure the records are described and held in a structure that is clear and preservable.

The records should be packaged under one top level folder with three component parts, as the below example illustrates. We refer to this as the 'Transfer Package'.
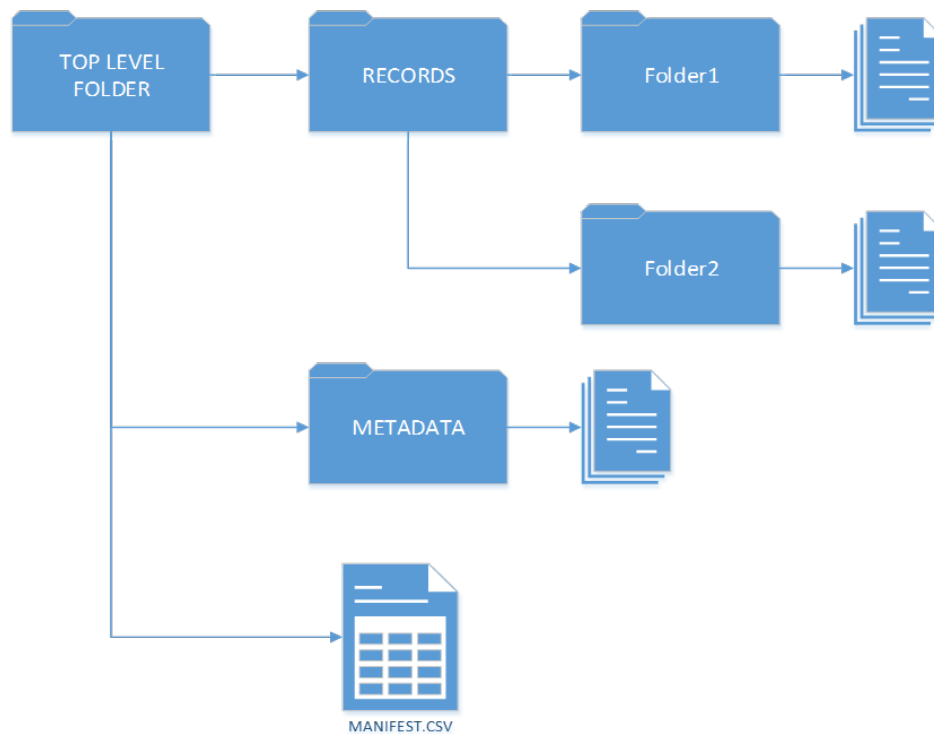
4.1   Top Level Folder

This folder contains the 'Records' folder, 'Metadata' folder and 'Manifest' csv file.

The folder should be named with the naming convention **YYYYMMDD-[Depositor Name]** (for example 20220412-ScottishGovernment). Please do not use spaces. The date listed should be the date on which you assembled the Transfer Package.

4.2   Records Folder

This folder contains all records selected for permanent preservation, as exported from your record keeping system. This folder can contain as many sub-folders as required and should follow the same folder names and structure as the originating system (as far as possible).

The folder should be named as **YYYYMMDD-[Depositor Name]-Records**.

4.3   Metadata Folder

When exporting records from the originating systems, there is a risk that some contextual information could be lost. The Metadata folder should include any technical or descriptive information that would aid the interpretation of the records.

This could include:

- Narrative description of what is included in the transfer.
- Metadata export from originating system of record.
- Indexes, keys or database schemas to interpret export.
- Screenshots from originating system that shows how the records were arranged and accessed.

There is no one-size-fits-all in respect of the metadata to supply as the format and need for this metadata can vary considerably depending on what is to be transferred and the system it derives from. Metadata requirements should be discussed with your Client Manager and the DRU ahead of transfer.

The folder should be named as **YYYYMMDD-[Depositor Name]-Metadata**.

4.4   Manifest CSV File

To ensure we have the necessary minimum descriptive information we require to interpret and preserve the records, we ask that a manifest file is assembled to accompany the records and metadata. In the short-term, this will allow us to confirm that what we have received is exactly what we expected to receive. In the longer-term, this assists us in cataloguing and helps to create a complete and reliable archival record for future users.

The manifest is a listing of each digital file that is contained in the Transfer Package. It should be formed as a csv (comma delimited file) that can be assembled and interpreted using spreadsheet applications (including Microsoft Excel).

The manifest will include descriptive (file name, pathway), technical (file format, checksum) and sensitivity (access status and conditions) information.

We strongly recommend using the software DROID to assemble the manifest csv file. A full explanation of how to use DROID can be found in Appendix C.

If it is not possible to download and install DROID, the DRU will provide guidance on how the Depositor or Depositor's IT support can put together the manifest manually. An overview of the expected minimum manifest fields is included in Appendix D.

The manifest file should be named as **YYYYMMDD-[Depositor Name]-Manifest.csv**

5.   TRANSFER

5.1   Notify NRS

Once your organisation is ready to transfer records to NRS, and you have prepared your records in accordance with section 4 above, please email a copy of the manifest csv file to the digital_records@nrscotland.gov.uk. The team will confirm the records described in the manifest are as expected and set a date for the transfer.

Our current method of transfer is via the NRS Managed File Transfer tool. This offers a secure method of transferring files person-to-person via a web browser, with an easy-to-use mailbox-type interface.

Further guidance on using this tool for transfer can be found in Appendix E.

Please do not delete the records from your systems until you have received formal notification from your Client Manager that it is safe to do so (see point 6.1).

5.2   Receipt of the Transfer Package by NRS

Once we have received the Transfer Package, it will be scanned for malware, profiled and validated against the manifest file to confirm the completeness of the records.

Once these processes are complete and the records have been transferred to our Digital Repository, we will confirm to your organisation that the transfer has been successful.

Should the transfer to NRS's Digital Repository fail in any way, a request will be made to the Depositor for a new Transfer Package to be sent.

6.   AFTER TRANSFER

6.1   Deletion of records

Records should, in most circumstances, be transferred to the archive at a point in their lifecycle when they are no longer required for ongoing business use. It is important that the version we store in our Digital Repository is the final version and there is no risk of the record being brought back into current business use and changed. It is therefore important that your organisation ensures that any copies of transferred records are managed appropriately to prevent this from happening: this is usually achieved by secure deletion. **This should only take place after your Client Manager has confirmed the transfer has been completely successful and the deletion may occur.**

6.2   Access to archival records

NRS can provide access to archival records by request via the NRS Managed File Transfer tool. Requests for access should be made to digital_records@nrscotland.gov.uk.

Access to records will only be permitted to third parties (other than the depositing organisation) if the records are classed as open; are not exempt under FOISA; and where no data protection considerations prevent access.

We also have a small amount of born digital records available online via Scotland's People. So far only Scotland's Cabinet Records (which were born digital in nature from 2005) are available via this portal, but we do hope to expand this to other born digital record sets in the future.

7.   FURTHER HELP

If you have any comments or queries on this guidance please contact the DRU at digital_records@nrscotland.gov.uk.

Further information on the management of born digital records can be found on our website at https://www.nrscotland.gov.uk/record-keeping/electronic-records-management.

8.   GLOSSARY

Born digital	Records that were created and used in a digital format.
Checksum	Computer generated sequence of letters and numbers that can be used to check data for errors. Sometimes referred to as a 'digital fingerprint'.

Client Manager	Key point of contact from NRS in arranging the deposit of records.
CSV	Comma Separated Value – a type of file that can be created easily in Microsoft Excel or other spreadsheet applications.
Digital Preservation	A series of managed processes and procedures which allow digital files to be kept and made available over time.
Encryption	A method of encoding digital files so that they are only readable by those with the relevant authorisation.
Lifecycle	The basic 'lifecycle' of a record, whether digital or paper, is creation, immediate business use, semi-current (mainly reference use in ongoing business), review and disposal. Selection for permanent preservation in an archive, is one disposal option.
Metadata	Descriptive, technical and contextual information about a digital file or series of files.

Appendix A.   Sensitivity Review

The contemporary nature of born digital records means that there is an increased likelihood of them containing sensitive content (whether personal, commercial or from a security perspective).

Records transferred to NRS are classed as either:

Open	accessible to the public at the point of transfer
Closed	not accessible to the public for a specified reason, and for a specified period.

In order to manage access to records over time, NRS requires a listing of sensitivity restrictions in records at the point of transfer. This should be recorded in the manifest file.

Identifying Sensitive Content

Record creators and users are best placed to review records for sensitivity.

It is very unlikely that an 'item-by-item' approach will be achievable, unless the records to be transferred are very low in volume. The review process is more likely to involve categorising and tagging records based on the purpose of their creation and use.

While we require the final review to be recorded in the manifest file, it is good practice for Depositors to maintain a record of sensitivity throughout the life of the records. Keeping a regularly updated record of sensitivity will prevent a time-consuming review process prior to transfer.

Recording Sensitivity Review in Manifest

We ask that the below fields be included in the manifest csv file, to record sensitivity in records transferred:

Manifest Field	Unit/Format Requirements	Comments
ACCESS_STATUS	CLOSED/OPEN	Whether or not the files will be open to public access from receipt by NRS. Your client manager can provide guidance on this.
ACCESS_CONDITIONS	If CLOSED, mandatory field. If OPEN, complete as N/A.	The reason why files are not open to public access. For example: Exempt under section 38(2)(c) OF FOISA

Manifest Field	Unit/Format Requirements	Comments
OPEN_FROM	If CLOSED, mandatory field in ISO 8601 Date Format. If OPEN, complete as N/A.	Date from which the closure ends. For example: 21230101

For guidance on where to include these fields in the manifest file, see Appendix C or D.

While each row of the csv file describes an individual digital item to be transferred, as noted above, it will likely only be feasible to review each item if the volume to be transferred is very low. It will likely be more practical to populate these fields by filtering or searching the listing and applying the correct classification for a defined group of records.

For further guidance on completing and recording the sensitivity review, contact your Client Manager.

Redaction

There are many reasons that a record may exist in a redacted form in the original record keeping system, but it is very unlikely that any sensitivity will exist indefinitely. **NRS will normally accept redacted records only so long as the original, un-redacted records are also included with the deposit**. This is so NRS can provide access to material once the sensitivity has lapsed.

You should make your Client Manager aware of any redacted material ahead of transfer.

Appendix B.   FILE FORMAT RESTRICTIONS

NRS will endeavour to accept files in the format they were originally created in and used, if possible. This is to maintain the archival integrity of the records.

There are, however, a small amount of file formats we do not accept:

- Executable program files of any type.
- Files with any encryption or password protection (this should be removed from files prior to transfer).
- Certain types of compressed files – such as zip files – that have been used to compress folders containing other files (these should be decompressed ahead of transfer).

You will note under Appendix E, that we do require the Transfer Package to be zipped and encrypted (for Closed records) prior to being transferred via the NRS Managed File Transfer tool. This is **only** for the purposes of transfer and the above points are referring to files and folders **within** the Transfer Package.

As part of our pre-transfer discussions, the DRU will ask what types of file formats you will be depositing and discuss any potential preservation risks with you.

Our broad principles for records that are 'preservable' are:

- Records that are not dependant on proprietary software to access (open formats)
    - OR the proprietary software is very commonplace such as Microsoft Word or Excel.
- Records that are not dependant on database applications to interpret. Database tables should be exported to open formats such as 'csv' prior to transfer.
- Multimedia formats (image, audio or video) where lossless compression is used over lossy compression.

Appendix C.   GENERATING MANIFEST USING DROID

DROID is a digital archiving tool developed by The National Archives (UK), specifically to obtain essential metadata for digital preservation. DROID can produce most of the manifest fields for you, with some minor manual additions required.

Instructions for installing DROID are available on The National Archives website:

https://www.nationalarchives.gov.uk/information-management/manage-information/preserving-digital-records/droid/

In the first instance, always contact your IT department before you attempt to install DROID. Most corporate IT departments prevent normal users from installing software and you will likely need their assistance.

C.1.   Applying correct settings to DROID:

Upon opening DROID, check that the 'Throttle' is set to 0.
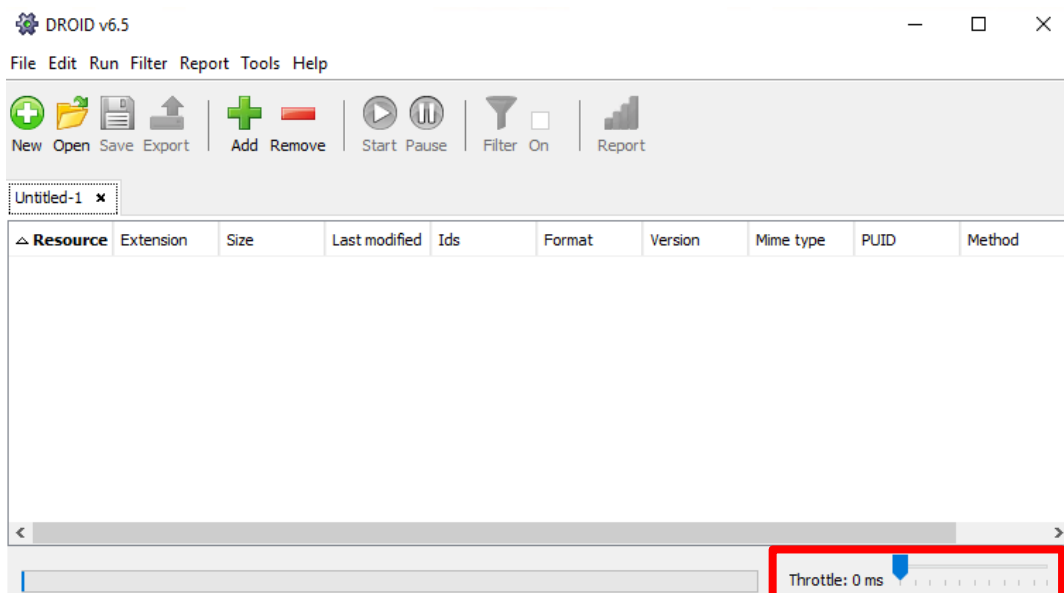
Click on 'Tools', then 'Preferences' and ensure the settings are as below:
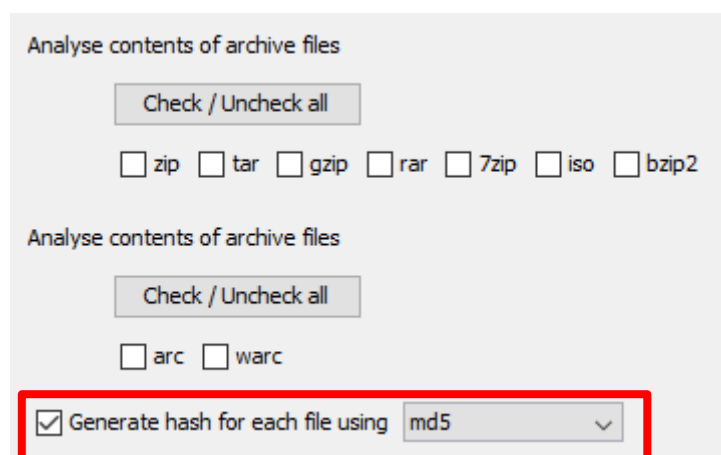
To apply preference changes to DROID, close tab 'Untitled-1' and select 'New'
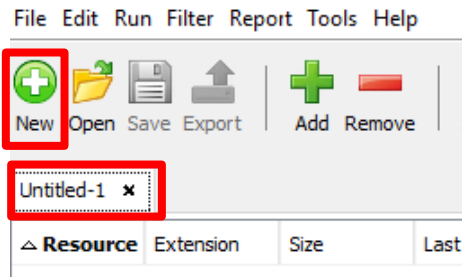
C.2.   Creating Profile:

To start generating the manifest file, select 'Add' and browse to the top level folder you wish to profile.
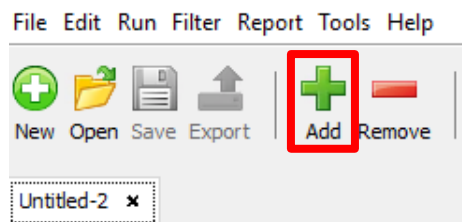
Select 'Start' from the top bar. A blue bar along the bottom of the screen will show progress. This may take several minutes depending on the size of the folder.

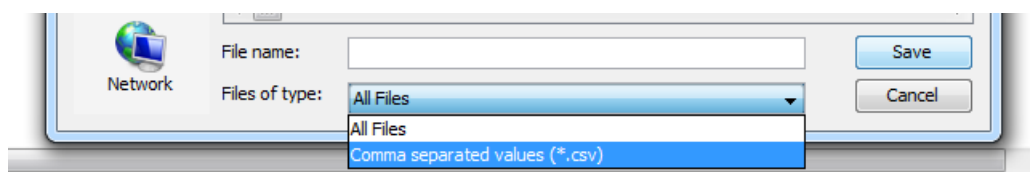Once complete, if you click on the top folder you will be able to see the results.

C.3.   Exporting DROID Profile as CSV:

To export the profile as a CSV file, select the 'Export' icon and ensure the settings are applied as below.
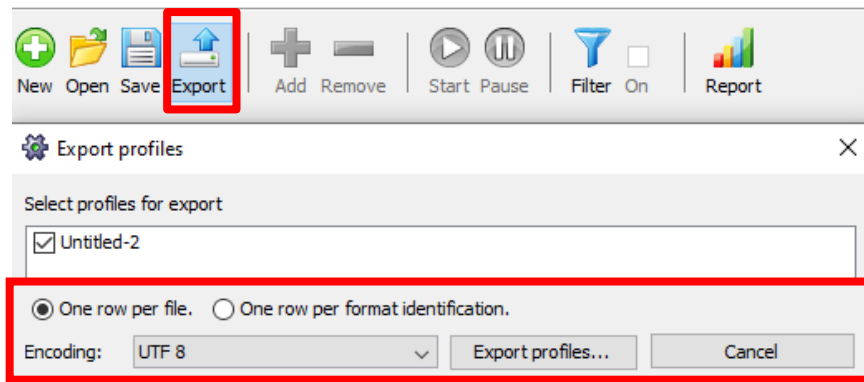
Ensure the '.csv' option is selected from the drop down menu and save the file using the naming convention 'YYYYMMDD-[Depositor Name]-Manifest.csv'

C.4.   Manually Adding Additional Columns to Manifest:

Open the manifest csv file in spreadsheet software, such as Microsoft Excel.

The data produced by DROID in columns A-R do not require any amendments but you should check this data looks complete. In particular, you should check column M 'MD5_Hash' contains checksums and is not empty. Checksums will only be listed for files and not folders.

Add 5 additional columns from column S and name as below:

Q	R	S	T	U	V	W
FORMAT_NAME	FORMAT_VERSION	ACCESS_STATUS	ACCESS_CONDITIONS	OPEN_FROM	RIGHTS	IDENTIFIER
Acrobat PDF 1.3 - Portable Document Format	1.3					

Description of how to complete columns S,T and U can be found in Appendix A: Sensitivity Review.

'RIGHTS' and 'IDENTIFIER' should be completed as below:

Manifest Field	Unit/Format Requirements	Comments
RIGHTS	Field to outline any copyright restrictions. If there are no copyright considerations known, complete as N/A.	For example: Covered by Crown copyright

Manifest Field	Unit/Format Requirements	Comments
IDENTIFIER	If unique identifiers exist in system of record, this field is mandatory. If no unique identifiers exist, complete as N/A.	This field should reflect what unique value the originating records system used to identify this file. This may be a reference ID or may be a unique pathway. Example 1: A1517671 Example 2: > Global Folder > File Plan > Administration > Management : April 2017 > Meeting Minutes > Note of Meeting

Appendix D.   GENERATING MANIFEST WITHOUT DROID (MINIMUM MANIFEST FIELDS)

We recognise that it is not always possible to install open source software to aid in the creation of the manifest. It may also be preferable to produce the manifest from an existing system or to put it together manually using spreadsheet software.

If this is the case, the Digital Records Unit will discuss this with you prior to the transfer and provide guidance on the best way to put this together, based on your system requirements and technical confidence.

As a guide, please refer to the below 10 minimum manifest fields we would expect to be included:

Manifest Field	Unit/Format Requirements	Comments
FILE_PATH	As arranged in Transfer Package.	Full folder pathway of each file to be transferred. If files originate from a system or database, this should be the pathway *after* the files have been exported, if this is different. For example: \20210916ScottishGovernment\20210916ScottishGovernmentData\Meeting_Minutes\Note of Meeting.pdf
NAME	Including extension if applicable.	Name of each file. For example: Note of Meeting.pdf
SIZE	Bytes	Size of each file in Bytes. For example: 34816
LAST_MODIFIED	ISO 8601 Date Format (YYYYMMDD).	Date the file was last modified. For example: 20210916
MD5_HASH	MD5 Checksum	Computer generated "digital fingerprint" for each file.

Manifest Field	Unit/Format Requirements	Comments
		For example: 095558938c10de958eabe0ff921295f5
ACCESS_STATUS	CLOSED/OPEN	Whether or not the files will be open to public access from receipt by NRS. Your Client Manager can provide guidance on this. For example: CLOSED
ACCESS_CONDITIONS	If CLOSED, mandatory field. If OPEN, complete as N/A.	The reason why files are not open to public access. For example: Exempt under section 38(2)(c) OF FOISA.
OPEN_FROM	If CLOSED, mandatory field in ISO 8601 Date Format. If OPEN, complete as N/A.	Date from which the closure ends. For example: 21230101
RIGHTS	Field to outline any copyright restrictions. If there are no copyright considerations known, complete as N/A.	For example: Covered by Crown copyright
IDENTIFIER	If unique identifiers exist in system of record, this field is mandatory. If no unique identifiers exist, complete as N/A.	This field should reflect what unique value the originating records system used to identify this file. This may be a reference ID or may be a unique pathway. Example 1: A1517671

Manifest Field	Unit/Format Requirements	Comments
		Example 2:
		> Global Folder > File Plan > Administration > Management : April 2017 > Meeting Minutes > Note of Meeting

Appendix E.   USING THE NRS MANAGED FILE TRANSFER TOOL

The NRS Managed File Transfer tool (MFT) provides NRS with a method to transfer files in a secure and controlled manner via SFTP, with an easy to use user interface that is accessed via a web browser.

Immediately prior to transfer via MFT the Depositor will need to:

- Add Transfer Package to zip file so it can be attached to email message. This will need to be created **after** the manifest file is assembled so that we can confirm the files are unaffected once we unpack the zip file. For transfer packages that contain Closed (sensitive) records, we would also require the zip file to be encrypted with AES-256 encryption.
- Once zip file is prepared, confirm the volume with the DRU (in gigabytes) so the DRU can ensure the transfer limits will meet the requirements for the transfer.

The DRU will send the request to transfer to the pre-agreed email account for the person conducting the transfer. This will come through as two emails from 'NRScotland Notification Service': one with your username and temporary password, and one with the link to attach your package. Reset your password and login to the tool.

You should see the request under your 'Inbox' as a message from the NRS Digital Archivist. Click on this message and drag and drop the zip file under 'Files'.
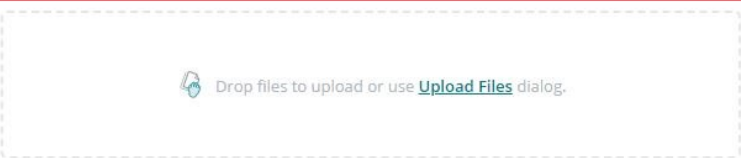
Select 'Send' and the package will be sent to the DRU.
Contact the DRU if you have any issues or queries on using this tool.